Method for monitoring microprocessor systems and stored-program controls

Patent Number: DE3502387
Publication date: 1986-07-31

Inventor(s): GREWE REINHOLD ING GRAD (DE); WRATIL PETER DIPL PHYS DR (DE)
Applicant(s): KLOECKNER MOELLER ELEKTRIZIT (DE)

Requested Patent: ☐ DE3502387
Application Number: DE19853502387 19850125
Priority Number(s): DE19853502387 19850125
IPC Classification: G06F11/30
EC Classification: G06F11/30
Equivalents:

Abstract

In this method, a control unit (1) is directly connected to the system bus of the microprocessor system (20) or of the stored-program control. The control unit compares checkpoints inserted in the safety-relevant area in the program paths with a stored map and outputs an error signal in the case of deviations. The control-unit (1) hardware construction differs from that of the central processing unit, which also operates with a different program. The checkpoints are determined by coordinates or other numbering and must be accurately defined by the control unit (1) by means of following information: a) identification of all checkpoints which follow the current checkpoint; b) the maximum time which may elapse until the next checkpoint is reached. The control unit compares this identification with the stored permissible identification and responds in the case of deviations. 

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Patentschrift**

(11) **DE 3502387 C2**

(51) Int. Cl.⁴: G06F 11/28

(21) Aktenzeichen: P 35 02 387.2-53
(22) Anmeldetag: 25. 1. 85
(43) Offenlegungstag: 31. 7. 86
(45) Veröffentlichungstag der Patenterteilung: 31. 3. 88

DE 3502387 C2

(73) Patentinhaber:

Klöckner-Moeller Elektrizitäts GmbH, 5300 Bonn, DE

(72) Erfinder:

Grewe, Reinhold, Ing.(grad.), 5200 Siegburg, DE;
Wratil, Peter, Dipl.-Phys. Dr., 5060 Bergisch Gladbach, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

DE-OS 32 25 712
DE 29 33 194 A1
EP 01 30 467 A2
IBM-TDB, April 1984, S. 6217-6220;

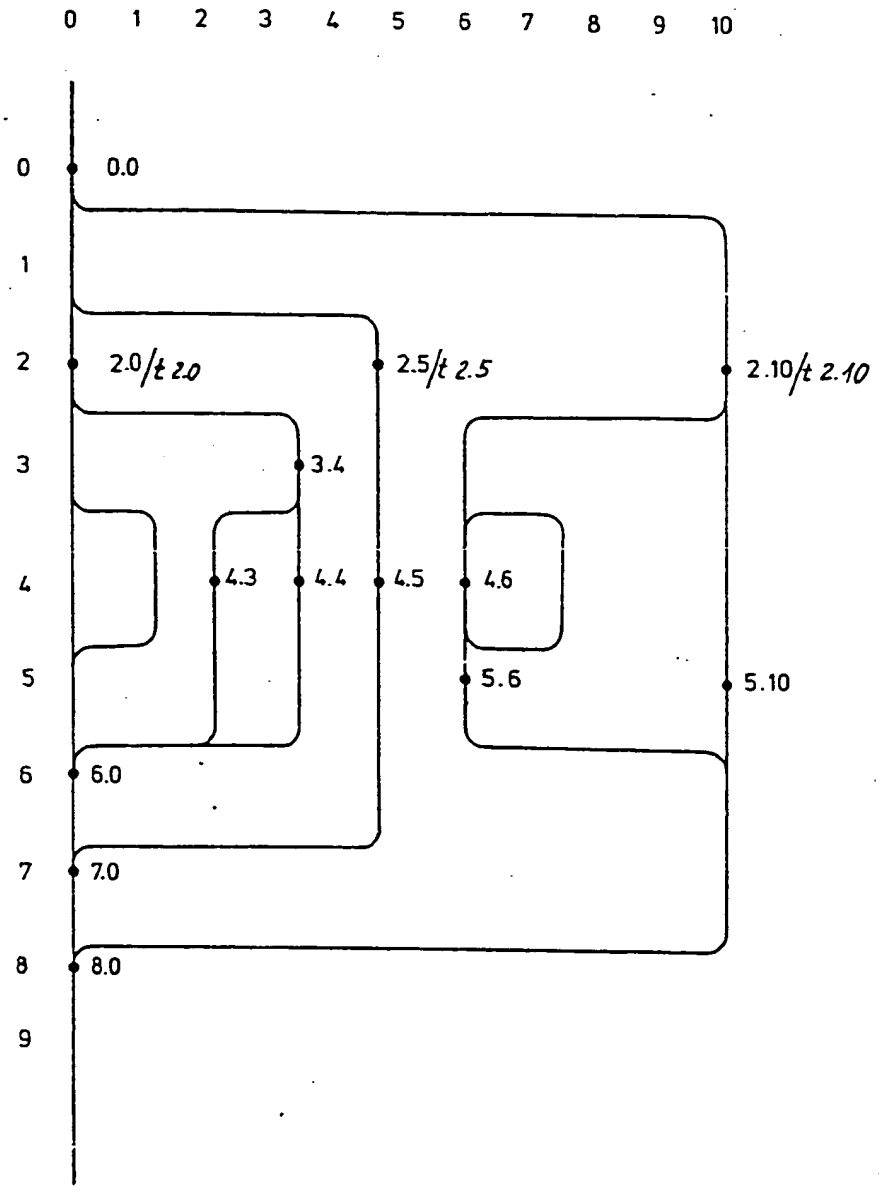
(54) Verfahren zur Überwachung von Mikroprozessorsystemen und speicherprogrammierbaren Steuerungen

DE 3502387 C2

ZEICHNUNGEN BLATT 1

Nummer: 35 02 387
Int. Cl.⁴: G 06 F 11/28
Veröffentlichungstag: 31. März 1988

Fig. 1



Patentansprüche

1. Verfahren zur Überwachung von Mikroprozessorsystemen und speicherprogrammierbaren Steuerungen, die zumindest eine Zentraleinheit enthalten, mittels einer Kontrolleinheit, die einen Speicher aufweist, in dem entsprechende Sollparameter gespeichert sind, die mit den Istwerten der im Programmablauf festpositionierten Kontrollpunkte verglichen werden, wobei die Kontrolleinheit mit direktem Zugriff auf den Systembus den Programmablauf einer oder mehrerer Zentraleinheiten überwacht und bei Abweichung des Istwertes von dem Sollwert die Zentraleinheit zu einer sicherheitsspezifischen Reaktion veranlaßt, **dadurch gekennzeichnet**, daß in einem sicherheitsrelevanten Bereich, der von der Zentraleinheit (2) durchlaufenen Programmpfade, frei wählbar vernetzte Kontrollpunkte eingebracht sind, deren Positions- und Zeitparameter im Speicher der Kontrolleinheit (1) als Sollabbild gespeichert sind und daß die Zentraleinheit (2) bei Erreichen eines Kontrollpunktes die aktuellen Positions- und Zeitparameter an die Kontrolleinheit (1) liefert, welche dort mit dem entsprechend gespeicherten Sollabbild auf Übereinstimmung verglichen werden, indem

a) kontrolliert wird, ob der aktuelle Kontrollpunkt von dem logisch richtigen Vorgängerkontrollpunkt angelaufen wurde und
b) eine Uhr in der Kontrolleinheit (1) gestartet wird die angibt, in welchem Zeitraum der nächste Kontrollpunkt angelaufen sein muß.

2. Verfahren nach Anspruch 1. dadurch gekennzeichnet, daß die Kontrolleinheit (1) hardwaremäßig unterschiedlich zur Zentraleinheit (2) aufgebaut ist.

3. Verfahren nach den Ansprüchen 1 und 2, dadurch gekennzeichnet, daß die Kontrolleinheit (1) mit einem zum Programm der Zentraleinheit (2) unterschiedlichen Programm arbeitet.

4. Verfahren nach den Ansprüchen 1 bis 3, dadurch gekennzeichnet, daß die fehlerfreie Arbeitsweise der Kontrolleinheit (1) selbst durch die Zentraleinheit (2) überwacht wird.

5. Verfahren nach den Ansprüchen 1 bis 4, dadurch gekennzeichnet, daß die Kontrolleinheit (1) eine eigene Stromversorgung aufweist, die bei Stromausfall eine ausreichende Pufferung erlaubt.

Beschreibung

Die Erfindung bezieht sich auf ein Verfahren zur Überwachung von Mikroprozessorsystemen und speicherprogrammierbaren Steuerungen, die zumindest eine Zentraleinheit enthalten, mittels einer Kontrolleinheit, die einen Speicher aufweist, in dem entsprechende Sollparameter gespeichert sind, die mit den Istwerten der im Programmablauf festpositionierten Kontrollpunkte verglichen werden, wobei die Kontrolleinheit mit direktem Zugriff auf den Systembus den Programmablauf einer oder mehrerer Zentraleinheiten überwacht und bei Abweichung des Istwertes von dem Sollwert die Zentraleinheit zu einer sicherheitsempfindlichen Reaktion veranlaßt.

Derartige Systeme bestehen aus einer oder mehreren Zentraleinheiten, die nach Vorschrift des Betriebs- oder Anwenderprogramm über ein Bussystem Komponenten ansteuern.

Für den richtigen Ablauf eines programmierten Prozesses ist die einwandfreie Funktion jeder Zentraleinheit eine notwendige Voraussetzung. Fehlerhafte Funktionen oder Zustände können, je nach Anwendung, zu gefahrvollen Situationen an dem zu steuernden Gerät für Mensch und Maschine führen. Derartige Fehlfunktionen müssen deshalb erkannt werden und zu einer sicheren Haltestellung des Gesamtsystems führen oder den Prozeß durch eine weitere Einheit fortführen lassen.

Zur Erfüllung dieser Sicherheitsanforderungen sind bereits Systeme bekannt, die mit zwei oder mehreren genau parallel geschalteten Schreib-Lese-Speichern ausgestattet sind, so daß alle Daten, die in den ersten Speicher geschrieben werden, auch in den folgenden Speichern enthalten sind. Beim Lesen werden die Daten der zusätzlichen Speicher auf einen Vergleicher geschaltet, der die gelesenen Daten mit dem ersten Speicher vergleicht und bei Ungleichheiten eine Fehlermeldung gibt. Damit auch bei gleichartiger Verfälschung der Daten in den Speichern ein Fehler erkannt wird, sind die Daten in den zusätzlichen Speichern invertiert abgelegt und werden auch beim Lesen wieder invertiert. Daher werden bei derartigen Sicherheitssystemen sowohl der Schaltungsaufbau als auch die Programmgestaltung sehr aufwendig.

Aus der DE-OS 29 39 194 ist ein Verfahren zum Überwachen des ordnungsgemäßen Ablaufs eines Programms bekannt, welches lediglich an den Übergabestellen der Unterprogramme ein Prüfbefehlswort aufweist, das benutzt wird, um die ihm zugehörige Parameterangabe als aktuellen Prüf-Ist-Befehl mit einer vorgegebenen Soll-Befehlsfolge in der Kontrolleinheit zu vergleichen. Nachteilig ist es hierbei, daß nur eine statische Positionskontrolle durchgeführt wird, bei der im Zuge des Programmablaufs lediglich festbestimmte Positionen, nämlich die Übergangsstellen von einem Unterprogramm zum folgenden Unterprogramm, überprüft werden. Dieses Verfahren ist nicht in der Lage eine verzweigte Pfadkontrolle in einem sicherheitsrelevanten Bereich, im Zuge der Programmabwicklung der aktuellen Unterprogramme durchzuführen, da die Kontrollpunkte nicht frei wählbar und vernetzt positioniert werden können. Fehlererkennung im zeitlichen Ablauf der Programmabwicklung sowie eine Kennung aller Kontrollpunkte, die auf den aktuellen Kontrollpunkt folgen können, ist bei dem Verfahren nach der DE-OS 29 39 194 nicht möglich.

In der Veröffentlichung "IBM Technical Disclosure Bulletin", April 1984, S. 6217 bis 6220 wird ein Verfahren beschrieben, das eine Aufzeichnung, der von der Zentraleinheit durchlaufenden Programmpfade und eine Ausgabe der im adressierten Speicher abgelegten Informationen ermöglicht. Hierfür enthält der Speicher ein festes Bitmuster, das in Abhängigkeit von einem Steuerbit über eine Output Control-Logic an einen Hardware-Monitor ausgegeben werden kann. Die Kontrollpunkte liegen in den von der Zentraleinheit zu durchlaufenden Programmpfaden. Nachteilig ist es bei diesem Verfahren, daß lediglich festbestimmte Informationen an den Hardware-Monitor gegeben werden, die dann zu einem späteren Zeitpunkt analysiert werden können. Fehler im zeitlichen Ablauf oder eine Ablaufunterbrechung zwischen den Kontrollpunkten, werden nicht erkannt.

In der EP-OS 01 30 467 wird ein Aufzeichnungsverfahren für Mikroprozessoren vorgestellt. Hierbei erfolgt, nach dem Programmdurchlauf, eine Zusammen-

führung der für den chronologischen Ablauf angelegten Aufzeichnungstabellen für jede Zentraleinheit in einem Mikroprozessorsystem. Hier wird lediglich eine Methode zur späteren Diagnose aufgezeigt. Dieses Verfahren bietet keine Fehlererkennung und entsprechende Sicherheitsreaktion während des aktuellen Programmdurchlaufs.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren zur Überwachung von Mikroprozessorsystemen und speicherprogrammierbaren Steuerungen zu schaffen, das in der Lage ist, den fehlerfreien Ablauf einer oder mehrerer Zentraleinheiten, synchron zum Prozeßablauf, zu kontrollieren, wobei die Kontrollpunkte frei wählbar und vernetzt in die Programmpfade eingebracht werden können und Fehlverhalten, insbesondere, die sich im zeitlichen Ablauf ergeben oder Ablaufunterbrechungen im Zuge des Programmdurchlaufs, zu erkennen und mittels einer Fehlermeldung eine sofortige sicherheitsspezifische Reaktion einleitet.

Diese Aufgabe wird erfindungsgemäß durch die kennzeichnenden Merkmale des Patentanspruchs 1 gelöst, während in den Ansprüchen 2 bis 5 besonders vorteilhafte Weiterbildungen des Verfahrens gekennzeichnet sind.

Damit systematische Fehler ausgeschaltet werden, ist der Schaltungsaufbau der zur Realisierung des Verfahrens verwendeten Kontrolleinheit unterschiedlich zu dem der zu überprüfenden Zentraleinheit. Ebenso ist das Prüfprogramm unterschiedlich zum Betriebs- und Anwenderprogramm aufgebaut, damit gleichartige Fehler im Prüfprogramm und im Betriebs- oder Anwendungsprogramm sofort erkannt werden. Auf diese Weise prüft die Kontrolleinheit den richtigen Ablauf der Zentraleinheit, während umgekehrt die Zentraleinheit die laufende Aktivität der Kontrolleinheit testet, so daß jeder Fehler oder Ausfall einer Einheit sicher erkannt wird.

Anhand der Zeichnung sei das Verfahren und eine beispielhafte Ausführungsform der Kontrolleinheit näher erläutert. Es zeigt

Fig. 1 ein Beispiel für den Programmablauf der Zentraleinheit mit den in die Pfadverzweigungen eingebrachten Kontrollpunkten nach dem erfindungsgemäßen Verfahren,

Fig. 2 den Informationsaufbau in einer Kontrolleinheit für den Programmablauf nach Fig. 1,

Fig. 3 das Blockschaltbild eines beispielhaften Aufbaus einer Kontrolleinheit zur Durchführung des erfindungsgemäßen Verfahrens.

In Fig. 1 ist ein Beispiel eines Programmablaufs der Zentraleinheit mit den in den Pfadverzweigungen eingebrachten Kontrollpunkten nach dem erfindungsgemäßen Verfahren dargestellt. Das Programm ist in einzelne verzweigte Programmpfade aufgeteilt, die in einer bestimmten Reihenfolge durchlaufen werden. In dem Programm sind die Kontrollpunkte 0.0 bis 8.0 in einem bestimmten Schema, das vom Anwenderprogramm und dessen Sicherheitsanforderungen bestimmt wird, angeordnet. Die Kontrollpunkte und die Kontrollpunktsituation sind durch das Koordinatensystem genau zu definieren. Eine andere Kennung, beispielsweise durch laufende Nummerierung, ist ebenso möglich.

Das erfindungsgemäße Verfahren besteht nun darin, daß eine Kontrolleinheit das richtige Anlaufen und Überlaufen der Kontrollpunkte in der vorgegebenen Zeit (oder Maximalzeit) kontrolliert und mit einem gespeicherten Sollabbild vergleicht. Dafür erhält sie für jeden Kontrollpunkt die folgenden Informationen:

a) Kennung aller Kontrollpunkte, die auf den aktuellen Kontrollpunkt folgen können;
b) die maximale Zeit, die bis zum Erreichen des nächsten Kontrollpunktes verstreichen darf.

Die Zentraleinheit gibt beim Überlaufen eines Kontrollpunktes dessen Kennung an die Kontrolleinheit weiter. Diese vergleicht die gemeldete Aktualkennung mit den, unter der letzten Kennung abgespeicherten, erlaubten Kennungen entsprechend dem Informationsaufbau, wie er in Fig. 1 dargestellt ist.

Als Beispiel seien hier die auf die Aktualkennung 0.0 folgenden Kontrollpunkte 2.0, 2.5, 2.10 herausgegriffen. Liegt nach 0.0 im Programmpfad als nächster Punkt 2.0 fest, so mit dieser Punkt in der Zeit t_{20} erreicht sein; bei 2.5 ist die Zeit t_{25} und bei 2.10 gehört zur Information die Zeit t_{210}.

Für die Zeitüberwachung enthält die Kontrolleinheit eine Uhr, die mit dem Erreichen eines Kontrollpunktes jeweils neu aufgezogen wird.

Die Kontrolleinheit erkennt einen Fehlerfall, wenn:

a) die gemeldete Kennung, hier die Koordinaten des Kontrollpunktes, nicht unter den abgespeicherten und erlaubten Kennungen zu finden ist, und
b) wenn die unter der letzten Kennung gespeicherte Zeit abgelaufen ist, ohne daß sich die im korrekten Ablauf folgende Kennung gemeldet hat.

Zur gegenseitigen Überprüfung sowohl der Zentraleinheit wie auch der Kontrolleinheit kann beim Erreichen jeder Kontrollpunktposition von den betroffenen Einheiten eine Quersummenrechnung oder eine andere fehlersignifikante Berechnung durchgeführt werden. Hierdurch kann die Zentraleinheit des Mikroprozessorsystems oder der speicherprogrammierbaren Steuerung immer wieder die korrekte Arbeitsweise der Kontrolleinheit überprüfen.

Fig. 3 zeigt ein Blockschaltbild eines beispielhaften Aufbaus einer Kontrolleinheit zur Durchführung des erfindungsgemäßen Verfahrens.

Die Kontrolleinheit 1 besteht aus dem Koordinatenspeicher, einem speziellen Halbleiterspeicher, der unter den Adressen die jeweils möglichen Folgepositionen enthält. Dieser Speicher wird vor dem Programmablauf geladen. Die Informationen vom Systembus erhält der Koordinatenspeicher über den Zwischenspeicher, der auch gleichzeitig die erforderlichen Informationen vom Systembus an den Kontrollprozessor liefert. Dieser hat die Aufgabe, das eigentliche Kontrollprogramm abzuarbeiten. Bei Feststellung eines Fehlers im Programmablauf erfolgt vom Kontrollprozessor eine Fehlersteuerung über den Systembus an die Zentraleinheit 2. Diese Fehlersteuerung kann aus der Mitteilung des Fehlers bestehen. Sie kann aber auch, je nach Art des Fehlers, eine Fehlerdiagnose enthalten. Der Kontrollprozessor gibt noch ein zweites Fehlersignal, das beispielsweise auf ein zweites System umschaltet, wenn das kontrollierte System ausfällt.

Zur Überwachung des zeitlichen Ablaufs ist eine unabhängige Uhr vorgesehen, welche bei Überlaufen eines Kontrollpunktes neu aufgezogen wird und zwar auf den Wert, der maximal zum Erreichen der nächsten Kontrollpunktposition erforderlich ist. In der Kontrolleinheit 1 ist noch ein Datenseparator, der eine Schalterfunktion ausübt, zwischen Koordinatenspeicher und Systembus angeordnet. Dieser Datenseparator regelt die Abfrage der Kontrollpunkte.

Damit die Kontrolleinheit von der Stromversorgung des Systems unabhängig ist, erfolgt eine separate Stromversorgung, die auch bei Spannungsabfall eine ausreichend lange Pufferung erlaubt.

Hierzu 3 Blatt Zeichnungen

Nummer: 35 02 387
Int. Cl.⁴: G 06 F 11/28
Veröffentlichungstag: 31. März 1988

Fig. 2

Aktual-Kennung	Folgepunkte		
0.0	2.0 / t	2.5 / t	2.10 / t
2.0	3.4 / t	6.0 / t	
2.5	4.5 / t		
2.10	4.6 / t	5.10 / t	
3.4	4.3 / t	4.4 / t	
4.3	6.0 / t		
4.4	6.0 / t		
4.5	7.0 / t		
4.6	4.6 / t	5.6 / t	
5.6	8.0 / t		
5.10	8.0 / t		
6.0	7.0 / t		
7.0	8.0 / t		
8.0	0.0 / t		

t = maximale Zeit zwischen Aktualkennung und Kennung eines Folgepunktes

Nummer: 35 02 387
Int. Cl.⁴: G 06 F 11/28
Veröffentlichungstag: 31. März 1988

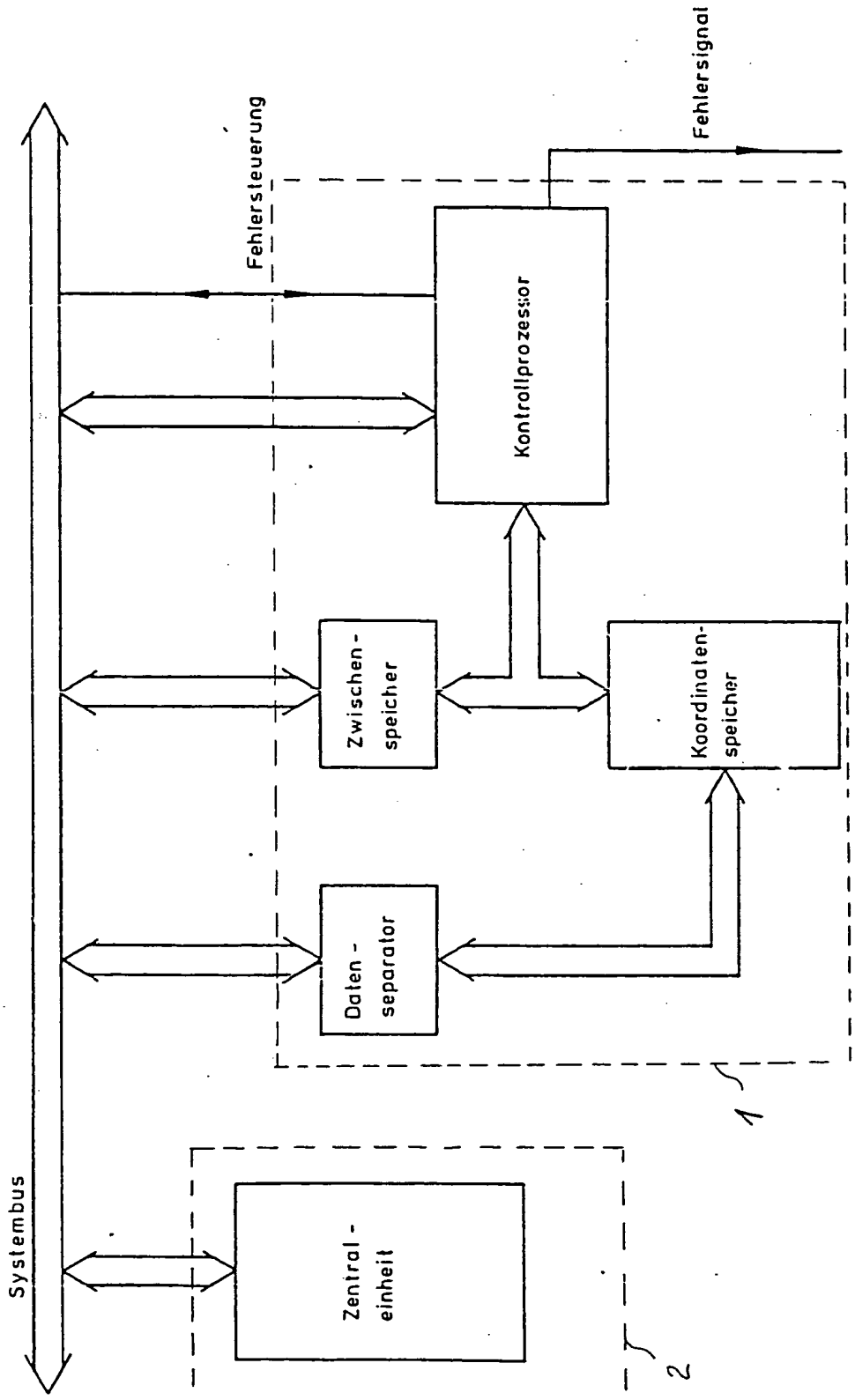


Fig. 3